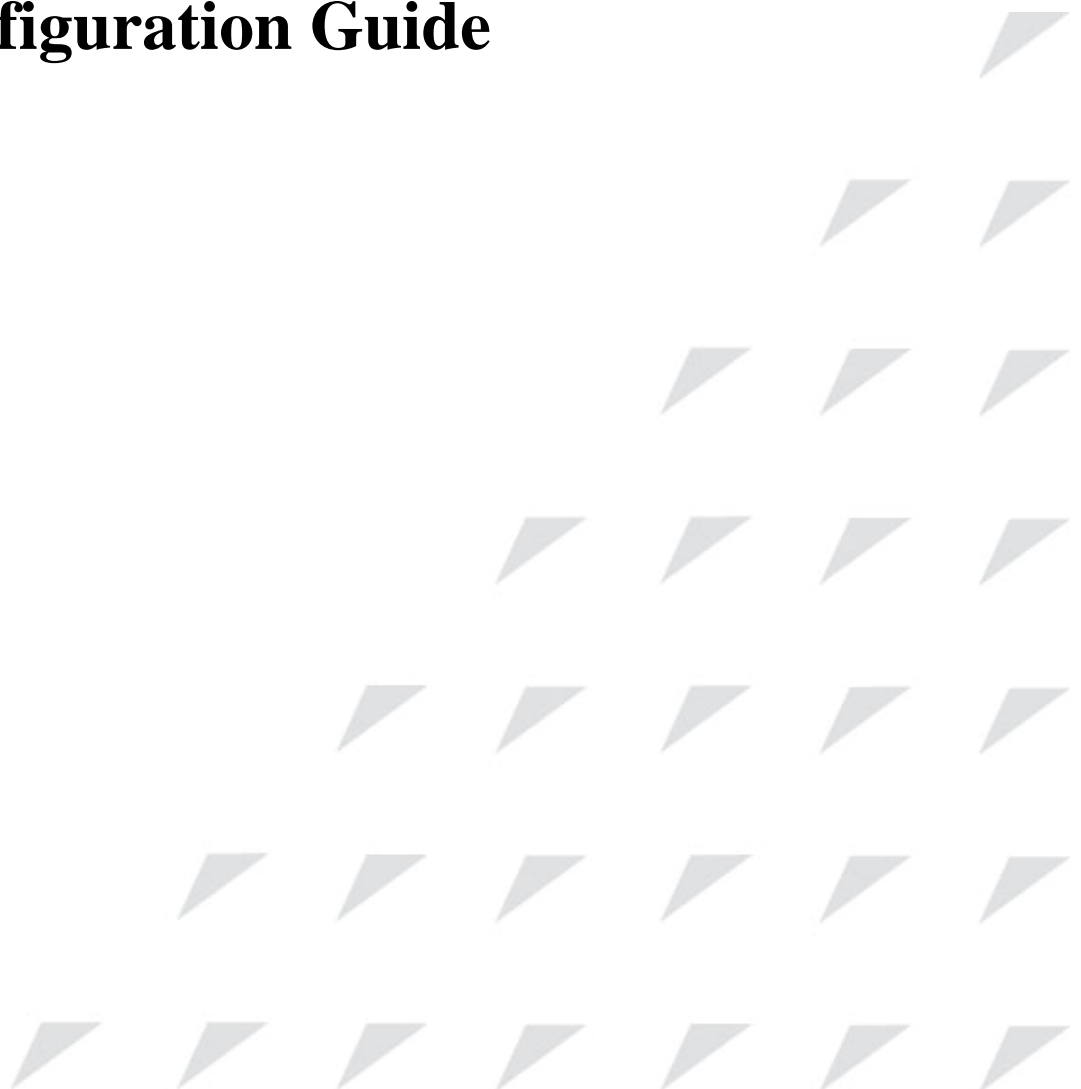


www.raisecom.com

SNMP Configuration Guide



Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2007 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

<http://www.raisecom.com>

Feedback

Comments and questions about how the ... system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

<http://www.raisecom.com/en/xcontactus/contactus.htm>.

If you have comments on the ... specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes	5
Chapter 1 SNMP Configuration Guide	1
18.1 SNMP principle	1
18.1.1 SNMP overview	1
18.1.2 SNMP V1/V2 interview	1
18.1.3 SNMPv3 interview	1
18.2 SNMPv1/v2/v3 management configuration	2
18.2.1 Default SNMP configuration	2
18.2.2 SNMPv1/v2 configuration	4
18.2.3 SNMPv3 configuration	5
18.2.4 SNMP v1/v2 TRAP configuration	8
18.2.5 SNMPv3 Trap configuration	9
18.2.6 Other SNMP configuration	9
18.2.7 Monitoring and maintenance	10
18.2.8 Typical configuration example	11

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ... device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《... User Manual》

《... Commands Notebook》

Organization

This manual is an introduction of the main functions of ... EMS. To have a quick grasp of the using of the EMS of ... , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 SNMP Configuration Guide

18.1 SNMP principle

18.1.1 SNMP overview

Now, the network management protocol that is the most extensively used in computer network is SNMP (Simple Network Management Protocol), which is also one of the standard protocol for Internet management.

On structure, SNMP is made up of agent and Network Management Station (NMS), or agent/management station mode. Among them, NMS is the workstation that runs the client program, the management workstations that is usually used now are IBM NetView and Sun NetManager; Agent means the server software that is running on the network equipment like the switch, management information base (MIB) is maintained in Agent.

When SNMP Agent receives the request message Get-Request, Get-Next-Request, Get-Bulk-Request that about MIB variable from NMS, Agent will take read/write operation to the MIB variable that NMS requested according to the message type, then create Response message according to the result, and send it to NMS as response.

On the other side, when SNMP Agent receives the message about some equipment's state like cold/warm booting or anomalous event, it will create a Trap message and send it to NMS actively and report these important incidents.

Raisecom serious SNMP Agent supports SNMPv1, SNMPv2 and SNMPv3

18.1.2 SNMP V1/V2 interview

SNMPv1 is a simple request/response protocol. The network management system sends out a request, the manager returns a response. The action is realized by one of the four protocol operations. The four operations are GET, GETNEXT, SET and TRAP. Through GET operation, NMS get one or more object (instance) values. If the agent can not offer all the request (instance) values from the request list, it will not offer any value. NMS use GETNEXT operation to get the next object instance value from the request list or the object list. NMS use SET operation to send commands to SNMP proxy and request re-configuration to the object value. SNMP proxy use TRAP operation to inform NMS the specific event irregularly.

Different from SNMPv1's simplex centralized management, SNMPv2 supports distributed/layered network management structure, in SNMPv2 management model some systems have both manager and proxy function; as proxy, it can receive the commands from senior management system, interview the local information stored, and offer the information summary of other proxy in the management domain that it charges, then send Trap information to senior manager.

18.1.3 SNMPv3 interview

SNMPv3 uses user-based security model. Whatever it is NMS sending query message to SNMP Agent, or SNMP Agent sending Trap message to NMS, the communication between NMS and SNMP Agent must be in the name of a certain user. Both SNMP NMS and proxy side maintains a local SNMP user table, user table record username, user related engine ID, if identification is needed

and the identification key, encryption information, so that it could make correct resolution to the message content and suitable response. SNMP user's configuration is to create key through the password information in the command lines, and add a user in local SNMP user table of the switch.

18.2 SNMPv1/v2/v3 management configuration

18.2.1 Default SNMP configuration

Function	Default value																
trap switch	Enabled																
The mapping relationship between SNMP user and visiting group	<div>The existed ones by default: initialnone、initial group</div> <table><thead><tr><th>Index</th><th>GroupName</th><th>UserName</th><th>SecModel</th></tr></thead><tbody><tr><td>-0</td><td>initialnone</td><td>raisecomnone</td><td>usm</td></tr><tr><td>1</td><td>initial</td><td>raisecommd5nopriv</td><td>usm</td></tr><tr><td>2</td><td>initial</td><td>raisecomshanopriv</td><td>usm</td></tr></tbody></table>	Index	GroupName	UserName	SecModel	-0	initialnone	raisecomnone	usm	1	initial	raisecommd5nopriv	usm	2	initial	raisecomshanopriv	usm
Index	GroupName	UserName	SecModel														
-0	initialnone	raisecomnone	usm														
1	initial	raisecommd5nopriv	usm														
2	initial	raisecomshanopriv	usm														
SNMP interview group	<div>The existed ones by default: initialnone、initial group</div> <div>Index: 0</div> <div>Group: initial</div> <div>Security Model: usm</div> <div>Security Level: authnopriv</div> <div>Context Prefix: --</div> <div>Context Match: exact</div> <div>Read View: internet</div> <div>Write View: internet</div> <div>Notify View: internet</div> <div>Index: 1</div> <div>Group: initialnone</div> <div>Security Model: usm</div> <div>Security Level: noauthnopriv</div> <div>Context Prefix: --</div> <div>Context Match: exact</div>																

	<p>Read View: system</p> <p>Write View: --</p> <p>Notify View: interne</p>
SNMP user	<p>The existed ones by default: raisecomnone、raisecommd5nopriv、raisecomshanopriv user</p> <p>Index: 0</p> <p>User Name: raisecomnone</p> <p>Security Name: raisecomnone</p> <p>EngineID: 800022b603000e5e00c8d9</p> <p>Authentication: NoAuth</p> <p>Privacy: NoPriv</p> <p>Index: 1</p> <p>User Name: raisecommd5nopriv</p> <p>Security Name: raisecommd5nopriv</p> <p>EngineID: 800022b603000e5e00c8d9</p> <p>Authentication: MD5</p> <p>Privacy: NoPriv</p> <p>Index: 2</p> <p>User Name: raisecomshanopriv</p> <p>Security Name: raisecomshanopriv</p> <p>EngineID: 800022b603000e5e00c8d9</p> <p>Authentication: SHA</p> <p>Privacy: NoPriv</p>
SNMP group	<p>The existed ones by default: public、private group</p> <p>Index CommunityName ViewName Permission</p>

	<pre> 1 public internet ro 2 private internet rw </pre>
The network administrator's contact information and logo	Contact information: support@Raisecom.com Device location : world china raisecom
SNMP object host address	None
SNMP figure	The existed ones by default: system、internet figure Index: 0 View Name: system OID Tree: 1.3.6.1.2.1.1 Mask: -- Type: included Index: 1 View Name: internet OID Tree: 1.3.6 Mask: -- Type: included

18.2.2 SNMPv1/v2 configuration

To protect itself and keep MIB from invalid visit, SNMP Agent brings in the idea of group. The management station in a group must use the group's name in all the Get/Set operations, or the request will not be taken.

The group name uses different character stream to sign different SNMP groups. Different groups may have read-only or read-write visit right. The group that has read-only right can only query the equipment information, while the group with read-write right can not only query the equipment information but also configure it.

When SNMPv1 and SNMPv2 takes group name authentication project, the SNMP message who's group name is not accorded will be dropped. The whole configuration steps are as follows:

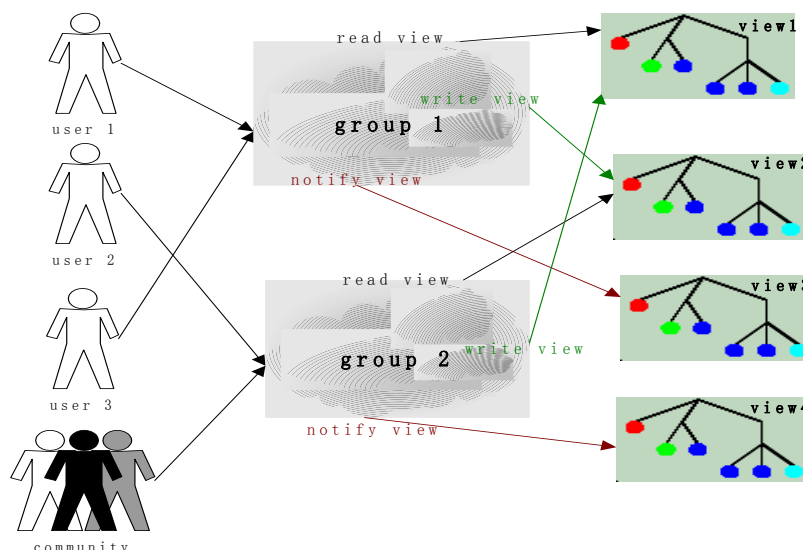
Step	Command	Description
1	config	Enter global configuration mode
(optical)	snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] {included excluded}	Define the figure and the contained MIB tree range; <i>view-name</i> figure name, the length can not exceed 32 character; <i>oid-tree</i> OID tree, OID number which the depth can not exceed 128; <i>mask</i> OID tree mask, the depth can not exceed 128, format is OID, each option of OID can be only 0 or 1;
2	snmp-server community <i>community-name</i> [view <i>view-name</i>] { ro rw }	Configure the community name and the relevant attributes. <i>view-name</i> : the view name ro: read-only rw: read-and-write
3	exit	Return to privileged EXEC mode
4	show snmp community	Show group information

⚠ Notice:

- Both SNOMPv1 and SNMPv2 takes group name authentication project, the SNMP message that is not accord with the group name that has been identified will be dropped.

18.2.3 SNMPv3 configuration

SNMPv3 takes USM (user-based security model) which is based on user's security safety model. USM brings the principle of interview group: one user or several users accord with a interview group, each interview group set the corresponding write, read, notify view, the user in interview group has the right in the figure. The interview group in which user send requests likeGet and Set must have the corresponding right, or the request will not be taken.



From the figure above, we can see that the normal interview to the switch for NMS, needs not only configuring the user but also making sure which group the user belongs to, the figure right that the interview group has and each figure. Complete configuration (including user's configuration) process is as follow:

Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server user <i>username</i> [remote <i>engineid</i>] [authentication { md5 sha } <i>authpassword</i>]	Add a user
3	snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { included excluded }	Define the view and its privilege of the MIB <i>view-name</i> specify the configured name of view <i>,oid-tree</i> specify OID tree <i>mask</i> the mask of OID sub-tree, each bit corresponds to a note of the sub-tree included means that the scale of the view includes all the MIB variables under OID tree excluded means that the scale of the view includes all the MIB

		variables out of OID tree
4	snmp-server group <i>groupname</i> user <i>username</i> { v1sm v2csm usm }	Configure the group which the user belongs to
5	snmp-server access <i>groupname</i> [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [context <i>contextname</i> [{ exact prefix }]] { v1sm v2csm usm } { noauthnopriv authnopriv }	<p>Define the access privilege of the group</p> <p><i>Groupname</i> is the name of access group;</p> <p><i>readview</i> is the read view, default is internet;</p> <p><i>writeview</i> is the write view, default is empty;</p> <p><i>notifyview</i> is informational view, default is empty;</p> <p><i>contextname</i> is the name of context or its prefix;</p> <p>exact prefix stands for the match type of the context name: exact means the input should be fully matched with the name of context, prefix means that only the first several letters should match with the name of context;</p> <p>v1sm v2csm usm are the security model, stands for SNMPv1 security model,SNMPv2 is the security model based on community and SNMPv3 is the security model based on the user respectively;</p> <p>noauthnopriv authnopriv is the security level, stands for no authentication and no encryption, or authentication without encryption respectively.</p>

6	exit	Exit to privileged configuration mode
7	show snmp group show snmp access show snmp view show snmp user	Show SNMP configuration information

18.2.4 SNMP v1/v2 TRAP configuration

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port mode
3	ip address A.B.C.D[A.B.C.D] vlanID	Configure the switch IP address A. B. C. D IP address [A. B. C. D] subnet mask vlanID vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	snmp-server host A.B.C.D version {1 2c} NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv1/v2 Trap object host A.B.C.D NMS IP address NAME SNMPv1/v2c group name <1-65535> receiving port number that object host receives Trap, by default it is 162;
6	exit	Return to privileged EXEC mode
7	show snmp host	Show configuration state

18.2.5 SNMPv3 Trap configuration

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port mode
3	ip address A.B.C.D [A.B.C.D] vlanID	Configure the switch IP address A.B.C.D IP address [A.B.C.D] subnet mask vlanID vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	snmp-server host A.B.C.D version 3 { noauthnopriv authnopriv } NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv3 Trap object host A.B.C.D HOST IP address NAME SNMPv3 username <1-65535> receiving port number that object host receives Trap, by default it is 162;
6	exit	Return to privileged EXEC mode
7	show snmp host	Show configuration state

18.2.6 Other SNMP configuration

1. Configure the network administrator label and contact access

The network administrator label and contact access sysContact is a variable of system group, its effect is to configure the network administrator label and contact access for management switch.

Step	Command	Description
1	config	Enter global configuration
2	snmp-server contact sysContact	Configure network administrator label and contact access
3	exit	Return to privileged EXEC

mode		
4	show snmp config	Show configuration situation

2. Enable/disable system sending trap message

Trap is used mainly for providing some switch important events to NMS. For example, when receiving a request with a fault group name and being allowed to send SNMP Trap, the switch will send a Trap message of failed authentication.

Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server enable traps	Allow the switch to send trap
3	exit	Return to privileged EXEC mode
4	show snmp config	Show the configuration

Use command **no snmp-server enable traps** to stop the switch from sending trap.

3. Configure the switch position

The switch position information sysLocation is a variable of MIB system group, which is used to describe the physical position of the switch.

Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server location <i>sysLocation</i>	Configure the switch position <i>sysLocation</i> specify the switch physical position, the type is character stream
3	exit	Return to privileged EXEC mode
4	show snmp config	Show the configuration

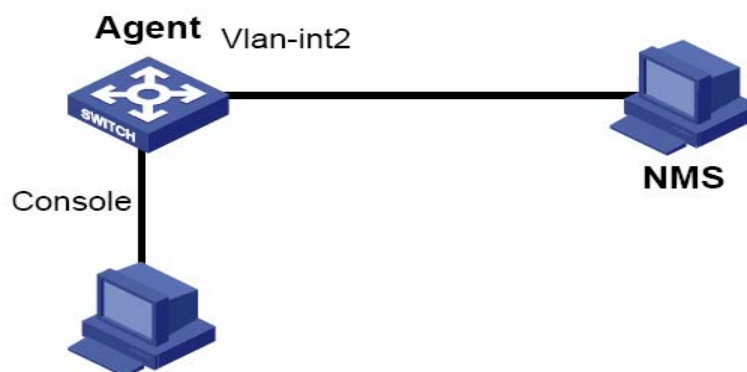
18.2.7 Monitoring and maintenance

Step	Command	Description
------	---------	-------------

1	show snmp community	Show SNMP community information
2	show snmp host	Show IP address of trap target host computer.
3	show snmp config	Show the SNMP engine ID, network administrator contact method, the position of the switch and whether TRAP is enabled.
4	show snmp view	Show view information
5	show snmp access	Show all the names of access group and the attributes of access group.
6	show snmp group	Show all the mapping relationship from user to access group.
7	show snmp user	Show the user information, authentication and encryption information.
8	show snmp statistics	Show SNMP statistics information

18.2.8 Typical configuration example

The interview control configuration example of V3:



First, set the local switch IP address to 20.0.0.10, user *guestuser1*, uses md5 identification algorithm, with the identification password raisecom, to interview the figure of MIB2, including all the MIB variable under 1.3.6.1.x.1, create guestgroup interview group, the safe mode safe model is usm, the safe grade is identified but not encrypted, the readable figure name is MIB2, thus the process of

guestuser1 mapping to interview group with the safe grade usm can be accomplished, and the result will be shown:

```

Raisecom#config
Raisecom(config)# interface ip 0
Raisecom(config-ip)#ip address 20.0.0.10 1
Raisecom(config-ip)#exit
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
Set successfully
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
Set successfully
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
Set successfully
Raisecom(config)#snmp-server group guestgroup user guestuser1 usm
Set successfully
Raisecom(config)#exit
Raisecom# show snmp access
  Index:          0
  Group:          initial
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      internet
  Write View:     internet
  Notify View:    internet

  Index:          1
  Group:          guestgroup
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      mib2
  Write View:     --
  Notify View:    internet

  Index:          2
  Group:          initialnone
  Security Model: usm
  Security Level: noauthnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:      system
  Write View:     --
  Notify View:    internet

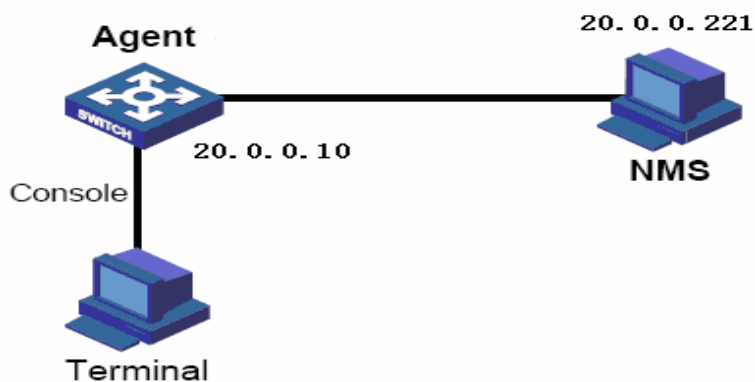
```

Raisecom# show snmp group

Index	GroupName	UserName	SecModel
0	guestgroup	guestuser1	usm
1	initialnone	raisecomnone	usm
2	initial	raisecommd5nopriv	usm
3	initial	raisecomshanopriv	usm

V3 Trap configuration example:

Trap is the information Agent sending to NMS actively, used to report some urgent events. As is shown below, set the switch IP address to 20.0.0.10, NMS host IP address to 20.0.0.221, username to raisecom, SNMP version v3, identified but not encrypted, all Trap



```

Raisecom#config
Raisecom(config)# int ip 0
Raisecom(config-ip)#ip address 20.0.0.10 1
Raisecom(config-ip)#exit
Raisecom(config)#snmp-server host 20.0.0.221 version 3 authnopriv raisecom
Raisecom#show snmp host
Index:      0
IP address: 20.0.0.221
Port:       162
User Name:   raisecom
SNMP Version: v3
Security Level: authnopriv
TagList:     bridge config interface rmon snmp ospf
  
```




北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>